Management System Description: Safeguards and Security

Management System Owner: John Sattler
Points of Contact: Pat Vent/Shaun Meadows

Issue Date: 09/10/2012
CB CMS Revision: 0

1.0 Purpose

The purpose of the EMCBC Safeguards and Security Management System is to assure that effective programs are in place for the protection of EMCBC interests from loss, damage, or other harm, whether intentional or unintentional. This includes assets in the possession or control of the EMCBC, supported small sites (without S&S staff), as well as third parties under various types of agreements with the EMCBC: management and operating (M&O) and non-M&O contracts, grants, cooperative agreements, Interagency Agreements, etc.

2.0 Responsibilities

The table below represents roles and responsibilities specific to this Management System. For a detailed description of CBC MS roles and responsibilities, please see the EMCBC Functions, Responsibilities and Authorities Document, PD-411-01,

Roles	Responsibilities
Director, EMCBC	• Responsible for management and implementation of Safeguards and Security(S&S) programs administered by EMCBC. • Serves as the EMCBC Head of Field Element and coordinates with the Department of Energy (DOE) Savannah River Operations Office as the Cognizant Security Authority (CSA) for programs, operations, and facilities under the purview of EMCBC to assure that effective safeguards and security programs are in place for the protection of EMCBC interests from loss, damage, or other harm, whether intentional or unintentional. EMCBC accomplishes these responsibilities through further assignments and delegated authorities within the organization, including Small Sites and outside the organization as described below.

Manager, Savannah River Operations Office	• Utilizing specific authorities assigned from EM-1, the Manager, Savannah River Site (SRS) is the CSA responsible and accountable to EM-1 for the safeguards and security program in accordance with the Atomic Energy Act and DOE Policy 470.1A.
Assistant Director, Office of Human Resources	• Support the implementation of the Homeland Security Presidential Directive (HSPD)-12 by performing the functions of Sponsors for Federal employees for the purposes of obtaining Federal Credentials (HSPD-12 Badges)
Assistant Director, Technical Services and Asset Management	• Assures S&S performance within previously established policy and clearly stated expectations within assigned organizational responsibilities (e.g., assigned EMCBC Cincinnati OH, Lakewood CO, and supported small sites that do not have qualified S&S staff). • Sets S&S expectations and assures performance of DOE Federal facilities under his/her purview (Cincinnati OH & Lakewood, CO). • Communicate regularly with the EMCBC Director, SRS CSA, as well as EM-44 and HS-90, on all S&S matters and performance, and develop and implement corrective actions, as appropriate. • In conjunction with the SR CSA, evaluates S&S performance under his/her respective operations (i.e. EMCBC Classification Office, EMCBC Telecommunications Security etc.). • TS&AM provides S&S program and contractor oversight support to Small Sites as requested by properly delegated FPD/FEM. Small Sites without delegated authorities will rely on the TS&AM.
Director, Safety & Quality Division	• Routinely communicates with SR and EM-44 on all EMCBC S&S matters and performance, and develops and implements corrective actions, as appropriate. • Serves as the CBC Management System Owner (MSO) and thus recommends final policy and program management activities to Director, EMCBC, AD, OTS&AM on matters affecting S&S performance within the EMCBC. • Supports properly delegated Small Site FPD/FEM.

EMCBC Site/Project Field Element Managers & Federal Project Directors	• Utilizing specific authorities assigned from EM or EMCBC, Site/Project Field Element Managers are the EM Line Managers responsible and accountable for the safety and protection of Federal and contractor employees, the environment, and the public at designated Sites/Projects. • Field Element Managers set contract S&S expectations and assure performance. • Field Element Managers ensure contractors develop and implement corrective action to matters pertaining to S&S. FEM's communicate with the EMCBC on S&S matters and performance as appropriate. • Field Element Managers, and if required, in conjunction with AD, TS&AM and SR CSA, evaluate S&S performance under their respective contracts.
EMCBC and supported small site S&S Staff (i.e., Federal staff of the EMCBC Classification Office/TS&AM, Safety & Quality Division/TS&AM and DOE WVDP)	• The EMCBC S&S staff supports the AD, OTS&AM and Small Site Field Element Manager &Federal Project Directors by providing technical and subject matter oversight in S&S related issues and other matters. This includes, but is not limited to, responsibility for pursuing personnel security clearances as needed, and implementing the Personnel Security Program for Federal and contractor employees at EMCBC and supported small sites. Small Sites with qualified S&S staff support their FEM/FPD and seek support from the EMCBC as needed. Currently, only the WVDP has qualified S&S staff. • Ensures appropriate S&S management requirements are placed into contracts. • S&S Staff will utilize the graded approach in assuring Safeguards and Security considerations are thoroughly integrated with all aspects of mission accomplishment and protection requirements are commensurate with the consequences of loss or misuse of the protected asset. • Coordinate with the applicable SR Program Point of Contact when the resources of the CSA are required to perform Federal assessment or contractor oversight or assessment.

3.0 Management System Operation

3.1 Overview

The EMCBC implements S&S programs and activities to protect its assets, human and physical, utilizing the principles and functions of DOE Policy 470.1A, Safeguards and Security Program. EMCBC staff:

1. Ensure that applicable safeguards and security management requirements are followed by EMCBC and supported sites personnel;
2. Ensure that appropriate safeguards and security management requirements are placed into contracts;
3. Provide oversight of contractor work planning and controls;
4. Integrate continuous feedback and improvement mechanisms into their work; and
5. Perform the necessary oversight/assessments of both the Federal staff and contractors.

This Management System addresses the training requirements for EMCBC personnel in the relevant aspects of S&S and performance of S&S functions that are Federal responsibilities. Furthermore, this Management System serves to ensure that EMCBC S&S requirements and methods of accomplishment are identified, communicated, and implemented by both EMCBC staff and contractors. This includes the oversight, assessment, and evaluation of both Federal staff and contractor performance and reporting of S&S performance data to EM and other DOE entities. Effective implementation of this Management System will promote the security and safety of EMCBC staff, contractor personnel, and the public, and protection of the environment.

The processes for addressing contractor S&S performance expectations are outlined in the individual contracts awarded by the EMCBC.

3.2 Key Functions/Services and Processes

3.2.1 EMCBC Safeguards and Security

This component includes a variety of formal and informal safeguards and security systems and processes for the protection and management of all EMCBC interests.

3.2.1.1 Program Management and Support

The EMCBC has several Federal Office facilities located in the Cincinnati, Ohio area and one in Lakewood, Colorado. These Offices are part of the EMCBC and as such, their S&S requirements are within the purview of the Assistant Director, Technical Services and Asset Management. Small Site Office/Projects are under the purview of a Field Element Manager of the Small Site Office/Projects, only the West Valley Demonstration Project has qualified S&S Federal oversight staff. Per DOE Directive (see Section 4.0 “Requirements”) the EMCBC serves as “Lead Responsible Office” for interests without qualified S&S staff and the WVDP serves as Lead for WVDP. Accordingly, Federal S&S staff members assigned to the EMCBC and the

WVDP is responsible for coordinating with the Cognizant Security Office (SR), which is responsible for:

- Approving all safeguards and security plans;
- Ensuring that the appropriate Foreign, Ownership or Influence (FOCI) determinations are made prior to allowing any classified work to occur;
- Ensuring appropriate facility clearances are granted and Facility Data and Approval Records (FDARs) and Contract Security Classification Specification (CSCS) forms are processed;
- Maintaining the Safeguards and Security Information Management System (SSIMS);
- Ensuring that safeguards and security surveys are conducted at facilities under their purview;
- Ensuring that any deficiencies identified during the surveys are corrected appropriately; and
- Approving/concurring on deviations to DOE Directives.

3.2.1.2 Protective Force

The WVDP Field Element Manager ensures that protective force personnel employed to protect DOE interests meet all requirements. No other small site or the EMCBC utilize Protective Forces.

3.2.1.3 Physical Security

Properly delegated Field Element Managers and the AD, TS&AM are responsible for acquiring any required vulnerability assessments and ensuring that adequate performance testing is conducted on physical security elements (not limited to barriers, locks, systems, and alarms), access controls, protective force operations, and transportation security.

3.2.1.4 Information Protection

The AD, TS&AM and properly delegated FEM have the responsibility for ensuring compliance in the areas of Classification, Operations Security (OPSEC), Communications Security (COMSEC), Classified Matter Protection and Control Program. Compliance with S&S requirements in these areas will achieve protection of classified, Unclassified Controlled Nuclear Information (UCNI) and Official Use Only (OUO) information and matter, ensuring that classified and sensitive activities conducted at facilities under the EMCBC purview are in accordance with the Atomic Energy Act and its implementing regulations (and related DOE Directives) and the National Industrial Security Policy. This necessitates the appointment of a DOE employee as FOCI Program Manager, COMSEC Program Manager, and a Facility Clearance Operations Manager. Appointees to these positions are individuals on the staff of the Cognizant Security Authority (SR) and are addressed in the Memorandum of Agreement (MOA) between SR and EMCBC. The EMCBC also has primary points of contact identified in the MOA with SR.

The responsibility to protect OUO information and matter is pertinent to all of the EMCBC supported small sites. Protection of UCNI is relevant to the WVDP and SPRU sites.

3.2.1.5 Cyber Security

The Office of Information Resource Management is responsible for implementing all cyber security mandates and guidance to ensure that cyber assets are adequately protected from unauthorized intrusion, disruption, damage, and destruction.

3.2.1.6 Personnel Security

In conjunction with Federal supervisors and the EMCBC Office of Human Resources, the TS&AM organization is responsible for pursuing personnel security clearances, when appropriately justified. The clearance requests for initial access authorizations, extensions, transfers, upgrades, downgrades, reinstatements, and reinvestigations will be routed through TS&AM to the Cognizant Personnel Security Office at SR. Eligibility decisions regarding personnel security clearances, including suspensions/revocations and denials, are accomplished in accordance with 10 CFR 710. HSPD Credentialing of Federal and cleared contractor staff is performed by the TS&AM.

3.2.1.7 Unclassified Visits and Assignments by Foreign Nationals

The EMCBC and Field Element Managers are responsible for the Unclassified Foreign Visits and Assignments Program consistent with the related DOE Directive. The Office of TS&AM will support Field Element Managers in executing their responsibility for assuring that the facilities under their cognizance comply with the appropriate requirements. This means assuring that as needed and in accordance with the Program requirements, unclassified foreign visits and assignments are: tracked in the Foreign Access Central Tracking System (FACTS); indices checks are favorably completed; security plans are completed; the visa/passport information is obtained; and appropriate subject matter expert reviews are completed.

3.2.1.8 Nuclear Materials Control and Accountability

Currently, no accountable nuclear materials are managed by the contractors under any of the small sites.

4.0 Requirements

4.1 Primary Responsibility

This Management System has primary responsibility for ("owns") the following requirements:

Document	Title
10 CFR 710	Criteria and Procedures for Determining Eligibility for Access to

Document	Title
	Classified Matter or Special Nuclear Material
10 CFR 810	Assistance to Foreign Atomic Energy Activities
10 CFR 1046	Physical Protection Of Security Interest
NRC 10 CFR 110	U.S. Nuclear Regulatory Commission Part 110—Export and Import of Nuclear Equipment and Material
DEAR 952.204-2	Security Requirements
DEAR 952.204-70	Classification/Declassification
DEAR 952.204-73	Facility Clearance
DoD 5220.22-M	National Industrial Security Program Operating Manual
DOE M 142.2-1	Manual For Implementation Of The Voluntary Offer Safeguards Agreement And Additional Protocol With The International Atomic Energy Agency
DOE O 142.2A	Voluntary Offer Safeguards Agreement And Additional Protocol With The International Atomic Energy Agency
DOE O 142.3A	Unclassified Foreign Visits and Assignments Program
DOE O 142.5	Committee on Foreign Investment in the United States
DOE M 200.1-1, Chapter 9 (restricted access)	Public Key Cryptography And Key Management (Unclassified)
DOE P 205.1	Departmental Cyber Security Management Policy
DOE M 205.1-3	Telecommunications Security Manual (Official Use Only)
DOE O 205.1B	Department Of Energy Cyber Security Program

Document	Title
DOE N 206.4	Personal Identity Verification
DOE N 251.87	Extension of DOE N 470.4, Reciprocal Recognition of Existing Personnel Security Clearances/Access Authorizations
DOE N 251.90	Extension of DOE N 470.5
DOE O 410.2	Management of Nuclear Materials
DOE O 452.8	Control of Nuclear Weapon Data
DOE O 457.1	Nuclear Counterterrorism
DOE M 457.1-1	Control Of Improvised Nuclear Device Information (Official Use Only)
DOE P 470.1A	Safeguards and Security Program
DOE O 470.3B	Graded Security Protection Policy
DOE M 470.4-4A, Change 1	Information Security Manual
DOE O 470.4B	Safeguard and Security Program
DOE O 471.1B	Identification and Protection of Unclassified Controlled Nuclear Information
DOE O 471.3, Admin. Change 1	Identifying and Protecting Official Use Only Information
DOE M 471.3-1, Admin. Change 1	Manual for Identifying and Protecting Official Use Only Information
DOE O 471.5	Special Access Programs
DOE O 471.6	Information Security
DOE O 472.2	Personnel Security
DOE O 473.3	Protection Program Operations

Document	Title
DOE O 474.2, Admin. Change 1	Nuclear Material Control and Accountability
DOE O 475.1	Counterintelligence Program
DOE O 475.2A	Identifying Classified Information
DOE O 5670.1A	Management And Control Of Foreign Intelligence
DOE CG-SS-4, Change 6	Classification and UNCI Guide for Safeguards and Security Information (Official Use Only)
E.O. 13467	Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information
DOC-EAR-0001	U.S. Department of Commerce - Export Administration Regulation
DOT-TFI-OFAC	U.S. Department of Treasury - Terrorism and Financial Intelligence, Office of Foreign Assets Control (OFAC)
DOS-ECR 121	U.S. Department of State Export Control Regulations International Traffic In Arms Regulations Part 121 - The U.S. Munitions List
NISP	National Industrial Security Policy
NSD 42	National Policy for the Security of National Security Telecommunications and Information Systems
NSDD 298	National Operations Security Program
OMB M-04-25	FY 2004 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
OMB M 04-26	Personal Use Policies and "File Sharing" Technology
P.L. 83-703 (68 stat. 919)	The Atomic Energy Act of 1954

4.2 Parsed Responsibility

This Management System is responsible for a part of the following high-level requirements:

Document	Title
OMB Circular A-130	Management of Federal Information Resources — Appendix III, Security of Federal Automated Information Resources
DOE O 206.1	Department of Energy Privacy Program — Appendix A, "Privacy Impact Assessments" and Appendix B, "Response and Notification Procedures for Data Breaches Involving Personally Identifiable Information"
OMB M-06-19	Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments — Not specified

5.0 Subject Area Program Descriptions, and Procedures

The following Subject Areas are maintained by this Management System:

- Program Management and Oversight Support
  - Procedure 1, Addressing and Identifying Foreign Ownership, Control or Influence (FOCI)
  - Procedure 2, Developing, Reviewing and Approving Site Security Plans (SSPs) and Site Safeguards and Security Plans (SSSPs)
  - Procedure 3, Terminating Registrations
  - Procedure 4, Appointing a Facility Security Officer (FSO)
  - Procedure 5, Establishing Access Authorizations (AA) for certain Key Management Personnel and Exclusions
  - Procedure 6, Conducting Assessments
- Personnel Security
  - Procedure 1, Requesting an Access Authorization (Clearance)
  - Procedure 2, Maintaining Security Awareness
  - Procedure 3, Implementing the Homeland Security Presidential Directive (HSPD-12)
  - Procedure 4, Requesting Classified Visits and SIGMA Access
- Information Security
  - Procedure 1, Managing A Classified Matter Protection and Control (CMPC) Program
  - Procedure 2, Managing a Field Classification Program
  - Procedure 3, Managing an Operations Security (OPSEC) Plan
  - Procedure 4, Implementing and Managing an Incident of Security Concern (IOSC) Program
  - Procedure 5, Review and Release of Information
- Unclassified Visits and Assignments by Foreign Nationals

- Procedure 1, Entering a Request into the Foreign Access Central Tracking System (FACTS)
- Procedure 2, Verifying Indices Check
- Procedure 3, Preparing a Specific Security Plan
- Procedure 4, Preparing a Cyber Security Plan
- Procedure 5, Routing the Visit or Assignment to the SME
- Procedure 6, Notifying the Host of a Foreign National Visitor's Approval

6.0 References

Document	Title
CNSS Instruction No. 1253	*Security Categorization and Control Selection for National Security Systems*
CNSS Policy No. 22	*Information Assurance Risk Management Policy for National Security Systems*
NSTISSI No. 1000	*National Information Assurance Certification and Accreditation Process (NIACAP)*
DOE CG-SS-6	*Classification and UCNI Guide for Safeguards And Security Information* (*Official Use Only*)
DOE M 205.1-5, Administrative Change 2	*Cyber Security Process Requirements Manual*
DOE M 205.1-6, Administrative Change 2	*Media Sanitization Manual*
DOE M 205.1-7, Administrative Change 2	*Security Controls for Unclassified Information Systems Manual*
DOE M 205.1-8, Administrative Change 2	*Cyber Security Incident Management Manual*
DOE G 226.1-1	*Safeguards and Security Oversight and Assessments Implementation Guide*
DOE G 241.1-1A	*Guide to the Management of Scientific and Technical Information*
DOE G 413.3-3	*Safeguards and Security for Program and Project Management*
DOE G 470.4-1	*Asset Protection Analysis Guide*
DOE G 471.3-1	*Guide to Identifying Official Use Only Information*
DOE G 473.2-1	*Guide for Establishment of a Contingency Protective Force*
DOE-STD-1171-2009	*Safeguard and Security Functional Area Qualification Standard*
Executive Order 13526	*Classified National Security Information*
Material Control and Accountability (MCA)	
"Unclassified Foreign National Visits and Assignments,"	Memorandum from Daniel B. Poneman, Deputy Secretary, to Distribution, dated 03/09/2010
"Security Incident (Including Cyber) Congressional Notification Protocol,"	Memorandum from Daniel B. Poneman, Deputy Secretary, to Heads of Departmental Elements, dated 06/24/2011

Document	Title
National Response Plan	
National Incident Management System (NIMS)	
National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 199	*Standards for Security Categorization of Federal Information and Information Systems*
NIST FIPS 200	*Minimum Security Requirements for Federal Information and Information Systems*
NIST FIPS 201-1, Change Notice 1	*Personal Identity Verification (PIV) of Federal Employees and Contractors*
NIST Special Publication (SP) 800-26	*Security Self-Assessment Guide for Information Technology Systems*
NIST SP 800-59	*Guideline for Identifying an Information System as a National Security System*
NIST SP 800-73-2	*Interfaces for Personal Identity Verification*
NIST SP 800-76-1	*Biometric Data Specification for Personal Identity Verification*
Office of Management and Budget (OMB) M-06-15	*Safeguarding Personally Identifiable Information*